

Übersicht Compliance Dokumente

1. Legal Data Hub - Schutz von Berufsgeheimnissen und personenbezogene Daten von Anfang an mitgedacht
2. Tüv Nord - Zertifikat ISO/IEC 27001 : 2022
3. Pentest Factory - Pentest Ergebnisse
4. Microsoft - Zusatzvereinbarung für Berufsgeheimnisträger

Legal Data Hub - Schutz von Berufsgeheimnissen und personenbezogenen Daten von Anfang an mitgedacht.



LDA Legal Data Analytics GmbH („LDA“) bietet maßgeschneiderte KI-Softwarelösungen für juristische Fachverlage, Content-Anbieter und Berufsträger:innen, um Fachinhalte effizient, strukturiert und in höchster Qualität zugänglich und nutzbar zu machen, um damit die tägliche Arbeit für Berufsträger:innen durch KI zu erleichtern. Mit der Kombination aus Technologie- und KI-Kompetenz sowie der Expertise aus der Branche für die Branche steht LDA für Professionalität, Verlässlichkeit, Vertrauen und Diskretion.

Vertrauen und Diskretion – berufsrechtliche Anforderungen einhalten

Berufsträger:innen der steuer-, wirtschafts- und rechtsberatenden Berufe sind zur Verschwiegenheit über alle ihnen in Ausübung ihres Berufs bekannt geworden und nicht offenkundigen Informationen verpflichtet (§ 43a BRAO, § 57 StBerG, u.a.). Die Verschwiegenheit von Berater:innen ist wesentliche Grundlage einer vertrauensvollen Zusammenarbeit von Mandanten und Berufsträgern. Die Verpflichtung zur Verschwiegenheit bezieht sich auch auf alle von Berufsträger:innen beschäftigten oder sonst für diese tätigen Personen und eingesetzten externen Dienstleister (§ 43e BRAO, §§ 62, 62a StBerG, u.a.).

Berufsträger:innen dürfen danach Dienstleistern Tatsachen, auf die sich die Verschwiegenheitsverpflichtungen beziehen, nur offenbaren, wenn die Offenbarung zur Inanspruchnahme der Dienstleistungen erforderlich ist (§ 43e Abs. 1 BRAO), der Dienstleister sorgfältig ausgewählt, in Textform zur Verschwiegenheit entsprechend den berufsrechtlichen Anforderungen verpflichtet, über die strafrechtlichen Folgen einer Pflichtverletzung belehrt (§ 203 StGB) und verpflichtet wurde, sich nur insoweit Kenntnis von Tatsachen und damit fremden Geheimnissen zu verschaffen, soweit dies für die Erfüllung des Vertrags erforderlich ist und nur weitere Dienstleister oder Personen zur Erfüllung des Vertrags heranzuziehen, soweit ihm dies gestattet und auferlegt wurde, auch diese Personen und Dienstleister zur Verschwiegenheit zu verpflichten.

Berufsträger:innen sind sich der berufsrechtlichen Verantwortung bewusst: Als Berufsträger:in entscheiden Sie sich mit LDA für einen Dienstleister, der die berufs-, datenschutz- und strafrechtlichen Anforderungen bereits bei der Entwicklung und Bereitstellung der KI-Systeme berücksichtigt und strukturell in der Unternehmens- und Systemarchitektur verankert hat. Berufsträger:innen, die in eigener Verantwortung ausschließlich erforderliche Informationen offenbaren, dürfen darauf vertrauen, dass die Nutzung des **Legal Data Hub** den **Compliance-Anforderungen** entspricht.

Aus der Branche für die Branche: Die Nutzung von KI-Systemen durch Berufsträger:innen kann unter Umständen die Offenlegung von Informationen („fremde Geheimnisse“) bedingen, die strengen rechtlichen, insbesondere berufsrechtlichen Anforderungen unterliegen. LDA ist ein geeigneter Dienstleister im Sinne von § 43e BRAO, § 62a BRAO u.a., sodass fremde Geheimnisse gegenüber LDA nicht „unbefugt offenbart“ werden. LDA erfüllt konsequent und nachgewiesen die Anforderung zur Verarbeitung personenbezogener Daten und „fremder Geheimnisse“, die Berufsträger:innen in Ausübung ihres Berufs erlangt haben.



Professionalität

Professionalität definiert sich nicht nur allein durch die Bereitstellung hochqualitativer und effizienter KI-Anwendungen. Gemeinschaftlicher Erfolg und der Einsatz effizienter und sicherer KI-Anwendungen, die Berufsträger:innen einen Mehrwert bieten, ist nur möglich, wenn LDA konsequent, transparent und wirksam die rechtlichen, insbesondere berufsrechtlichen Anforderungen umsetzt. **LDA und der Legal Data Hub erfüllen die Compliance-Anforderungen.**

Legal Data Hub – Auszug der technischen und organisatorischen Maßnahmen

Anforderung	Rechtsquelle	Umsetzung
LDA stellt einen Auftragsverarbeitungsvertrag (AVV) bereit, der den Anforderungen der Art. 28, 29 DSGVO entspricht.	§ 2 Abs. 2 BORA § 43e Abs. 2 BRAO („sorgfältig“) Art. 28 DSGVO	✓
LDA verarbeitet Informationen und personenbezogene Daten ausschließlich zu den nach dem Vertrag definierten und nicht zu eigenen Zwecken („ Zweckbindung “).	§ 43e Abs. 1 BRAO („erforderlich“) § 43e Abs. 2 BRAO („sorgfältig“) Art. 5, 6 DSGVO Art. 29 DSGVO	✓
Kein KI-Training: Der LDA offenbarte und offengelegte Informationen und personenbezogenen Daten werden nicht für das Training von KI-Systemen verwendet.	§ 43e Abs. 1 BRAO („erforderlich“) § 43e Abs. 2 BRAO („sorgfältig“) Art. 5, 6 DSGVO Art. 28 DSGVO	✓
LDA setzt ausschließlich genehmigte Unterauftragsverarbeiter für die Bereitstellung der Anwendungen ein. Die Unterauftragsverarbeiter unterliegen denselben Pflichten wie LDA gegenüber den Berufsträger:innen.	§ 203 Abs. 3 StGB § 43e Abs. 3 Nr. 3 BRAO Art. 28 Abs. 3 DSGVO Art. 28 Abs. 4 DSGVO	✓
LDA hat sämtliche bei ihr beschäftigten, für sie sonst tätigen Personen und Dienstleister, insbesondere Unterauftragsverarbeiter, zur Verschwiegenheit verpflichtet und zu den strafrechtlichen Folgen einer Pflichtverletzung belehrt.	§ 203 Abs. 4 StGB § 43e Abs. 2 BRAO („sorgfältig“) § 43e Abs. 3 BRAO („Vertrag“)	✓
LDA verfügt über ein wirksames Datenschutz- und Informationssicherheitsmanagementsystem . LDA ist nach ISO/IEC 27001:2022 zertifiziert. Die eingesetzten Unterauftragsverarbeiter sind zertifiziert nach ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018: ISO/IEC 27701, u.a. und verfügen über ein BSI C5-Testat.	§ 2 Abs. 2 BORA § 43e Abs. 2 BRAO („sorgfältig“) Art. 5, 6, 28, 29 DSGVO	✓
LDA und die von ihr eingesetzten Unterauftragsverarbeiter haben angemessene technische und organisatorische Maßnahmen zum Schutz der Informationen und personenbezogenen Daten getroffen.	§ 2 Abs. 2 BORA § 43e Abs. 2 BRAO („sorgfältig“) Art. 5, 6, 28, 29 DSGVO Art. 32 DSGVO	✓
LDA verarbeitet personenbezogene Daten und Informationen ausschließlich in der Europäischen Union und den Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum („ EWR “), insbesondere in Deutschland .	§ 43e Abs. 4 StGB Art. 44 ff. DSGVO	✓

Zertifikat

für das Managementsystem nach
ISO/IEC 27001 : 2022

Die Zertifizierungsstelle TÜV NORD CERT GmbH bestätigt hiermit als Ergebnis der Auditierung, Bewertung und Zertifizierungsentscheidung gemäß ISO/IEC 27006:2015/Amd.1:2020, dass die Organisation

LDA Legal Data Analytics GmbH
Hochwaldstraße 26
81377 München
Deutschland



ein Managementsystem konform zu den Anforderungen der ISO/IEC 27001 : 2022 betreibt und innerhalb der Laufzeit des Zertifikats von 3 Jahren auf Konformität überwacht wird.

Geltungsbereich

Entwicklung und Betrieb von Software

Unter Berücksichtigung der SoA v.9 vom 10.04.2025

Zertifikat-Registrier-Nr. 44 121 242212
Auditbericht-Nr. 3538 5642

Gültig von 2025-06-10
Gültig bis 2028-06-09
Erstzertifizierung 2025

Essen, 2025-06-10

Zertifizierungsstelle der TÜV NORD CERT GmbH



Nutzen Sie unsere
Datenbank, um die
Zertifikatsgültigkeit zu
verifizieren.

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen
www.tuev-nord-cert.de

TÜV®



Deutsche
Akkreditierungsstelle
D-ZM-12007-01-00

1. Client Notification: Penetration Test

This document summarizes the results of a performed penetration test for LDA Legal Data Analytics GmbH (in the following also called „LDA“). The purpose of the penetration test was to gain an overview of the current security status of the „OS Assist“ web application and its underlying IT infrastructure. The goal was to identify vulnerabilities, give an overview of the identified findings and to give a recommendation for minimizing these risks.

The following tests were included in the project scope:

- » **Penetration test of web applications:** From the perspective of an external attacker with and without access credentials (grey-box), including an automated vulnerability scan.
 - Pentest-ID: LDAPT-2
 - Scope: OS Assist web application and associated IDP authentication flows
 - Application URL: <https://dev.os-assist.de>
 - IDP URLs: <https://online.otto-schmidt.de>, <https://anmeldung.otto-schmidt.de>
 - Testing period: 21.07.2025 to 24.07.2025

1.1. Risk Assessment – Web Application



The illustration on the left represents the overall risk of the analyzed test object and is based on the highest risk rating "**MEDIUM**" of an identified finding.

During the pentest, no vulnerabilities with a high, or critical risk were identified. However, vulnerabilities with a low to medium risk exist, for which we recommend remediative measures.

Pentest Factory GmbH
Frankfurt am Main – 24.07.2025

Andres Rauschecker
[Senior Penetration Tester]

Laurent Vetter
[Team Lead Pentesting, ppa.]

2. Assignment and Background

2.1. Project Background

LDA wants to ensure confidentiality, integrity and availability of IT-assets within their IT-infrastructure. To determine the current security level of the „OS Assist“ web application, Pentest Factory GmbH was hired to perform a penetration test.

2.2. Project Goal, Scope and Methodology

The objective of this penetration test was to identify potential security vulnerabilities that could impact the confidentiality, integrity and availability of information processed by the „OS Assist“ web application and underlying IT infrastructure.

Penetration Test of Web Applications

The penetration test included a comprehensive security analysis of the “OS Assist” web application at the network and application level. Our tests at the network level included an automated vulnerability scan as well as a manual analysis of all network services provided by the application server from the perspective of an external attacker (black box). The application-level tests were performed using a semi-manual approach with and without valid user access credentials (grey-box).

2.3. Applied Methodologies for Penetration Tests

When carrying out penetration tests, Pentest Factory GmbH follows the proven test specifications of OWASP and OSSTMM.

Within infrastructure tests, the following tests were performed:

- » Passive analysis of publicly available information about the target organization
- » Identification of available network services and manual security analysis
- » Automated vulnerability scans of the target infrastructure and verification of findings

For application testing, all typical tests described in the OWASP Testing Guide (Version 4) ¹ have been performed, including:

- » Information gathering
- » Testing configuration and deployment management
- » Identity & Access Management (IAM), Session and Authentication testing
- » Input and output validation tests
- » Privilege escalation, cryptography, error handling and plausibility checks

¹ https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

Microsoft Customer Agreement

Zusatzvereinbarung für Berufsgeheimnisträger

Diese Zusatzvereinbarung wird wirksam, wenn der Kunde sie annimmt („Annahme“) und läuft ab entweder (i) am Ablaufdatum des Microsoft Kundenvertrages oder (ii) am letzten Tag des Monats, 36 volle Kalendermonate nach der Annahme des Kunden, je nachdem, welches Datum das frühere ist.

Die Parteien vereinbaren, die folgenden neuen Abschnitte in den Microsoft Kundenvertrag aufzunehmen:

Berufsgeheimnisträgerklausel

Microsoft ist bewusst, dass rechtliche Verpflichtungen hinsichtlich der Gestattung des Zugriffs auf Informationen von Mandanten des Kunden bestehen und die Verletzung solcher Verpflichtungen strafrechtliche Folgen für die Beteiligten haben kann (vgl. insbesondere §§ 203, 204 StGB) (Freiheits- oder Geldstrafe).

Microsoft ist gemäß der zwingend anwendbaren gesetzlichen Bestimmungen zur Verschwiegenheitspflicht und den mit dem Kunden bestehenden Vertragsbestimmungen zur Verschwiegenheit verpflichtet.

Microsoft wird verpflichtet, die zur Verfügung gestellten Kundendaten nicht in einem anderen als dem vertraglich beschriebenen Umfang zu nutzen. In diesem Zusammenhang wird Microsoft im Rahmen der Verarbeitung zur Bereitstellung der Onlinedienste für den Kunden insbesondere verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Unter „sich Kenntnis verschaffen“ verstehen die Parteien den Vorgang der kognitiven, menschlichen und inhaltlichen Kenntnisnahme (z. B. Zugriff auf Inhalte einzelner Dokumente mit dem Ziel diese kognitiv, menschlich und inhaltlichen zur Kenntnis zu nehmen).

Microsoft und Microsofts Subunternehmer dürfen weitere Personen zur Bereitstellung der Onlinedienste einsetzen. Microsoft stellt sicher, dass sowohl die von Microsoft eingesetzten Personen, soweit sie im Zusammenhang mit ihrer Tätigkeit Kenntnis von zur Verfügung gestellten Kundendaten erlangen könnten, als auch die Subunternehmer gemäß der mit dem Kunden bestehenden Vertragsbestimmungen zumindest in Textform zur Verschwiegenheit verpflichtet sind und dass auch die Subunternehmer verpflichtet sind, die von diesen eingesetzten Personen entsprechend zu verpflichten.